The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) A method of transmitting an authentication message in a switching Fabric, comprising:

ascertaining if the authentication message has a length that exceeds the message length supported by a target entity; and either:

fragmenting the authentication message into message fragments if the length of the message exceeds the message length supported by the target entity; and sequentially sending the message fragments one by one across the Fabric; or

sending the authentication message in its entirety if the length of the authentication message is less than the message length supported by the target entity.

2. (Original) The method of claim 1, wherein fragmenting the authentication message into message fragments further comprises setting a fragmentation bit in each message fragment except the last message fragment.

3. (Original) The method of claim 2, wherein the setting of the fragmentation bit of one of the message fragments indicates that a subsequent message fragment is to be sent.

4. (Original) The method of claim 1, wherein fragmenting the authentication message into message fragments further comprises resetting a fragmentation bit in the last message fragment of the authentication message.

5. (Original) The method of claim 1, wherein fragmenting the authentication message into message fragments further comprises labeling each message fragment with a Sequence Number.

6. (Original) The method of claim 4, wherein the resetting of the fragmentation bit in the fragmentation field of the last message fragment indicates that no subsequent message fragments will follow the last message fragment.

7. (Original) The method of claim 1, wherein the message comprises, but is not limited to, authentication information and contains one or more of the following fields:

a field that identifies the authentication message as an authentication message; and

an authentication command code field that identifies the particular authentication message of an authentication protocol.

8. (Original) The method of claim 6, wherein the authentication protocol comprises but is not limited to the following protocols: DH-CHAP, SRP, or FCAP.

9. (Original) The method of claim 1, wherein the target entity is an end device in the Fabric.

10. (Original) The method of claim 1, wherein the target entity is the Fabric.

11. (Original) The method of claim 6, wherein the target entity either accepts or discards the message fragment based on the value of the Sequence Number.

12. (Original) An authentication method to authenticate an initiating entity seeking to access a target entity, comprising:

ascertaining at the initiating entity if an authentication message has a length that exceeds the message length supported by the target entity; and either:

fragmenting the authentication message into message fragments if the length of the message exceeds the message length supported by the target entity and sequentially sending the message fragments one by one over a Fibre Channel Extended Link Service to the target entity; or

sending the authentication message in its entirety to the target entity over a Fibre Channel Extended Link Service if the length of the authentication message is less than the message length supported by the target entity.

13. (Original) The method of claim 12, wherein the fragmenting the authentication message into message fragments by the initiating entity further comprises setting a fragmentation bit in each message fragment except the last message fragment.

14. (Original) The method of claim 13, wherein the setting of the fragmentation bit of one of the message fragments indicates that a subsequent message fragment is to be sent by the initiating entity.

15. (Original) The method of claim 12, wherein fragmenting the authentication message into message fragments further comprises resetting a fragmentation bit in the last message fragment of the authentication message.

16. (Original) The method of claim 12, wherein fragmenting the authentication message into message fragments further comprises labeling each message fragment with a Sequence Number.

17. (Original) The method of claim 16,

receiving the message fragments at the receiving entity;

ascertaining the value of the Sequence Number for each of the received fragments, and either:

accepting the content of the message fragment if the received Sequence Number is different than the Sequence Number carried in the previously received message fragment; or

discarding the content of the message fragment is the received Sequence Number is equal to the Sequence Number carried in the previously received message fragment.

18. (Original) The method of claim 16,

receiving the message fragments at the receiving entity;

ascertaining the status of a fragmentation bit for each of the received fragments, and either

receiving at least one more of the message fragments at the receiving entity if the fragmentation bit for the most recently received message fragment is set; or

not receiving additional message fragments associated with the authentication method at the receiving entity if the fragmentation bit for the most recently received message fragment is reset.

19. (Original) The method of claim 18, wherein the receiving entity interprets the reset fragmentation bit of the most recently received message fragment of the authentication message as either:

the authentication message is only one message fragment long; or

the most recently received message fragment is the last fragment of the authentication message that is more than one message fragment long.

20. (Original) The method of claim 12, further comprising the target entity sending a second authentication message to the initiating entity in response to the authentication message.

21. (Original) The method of claim 20, wherein the target entity sends the second authentication message to the initiating entity in response to the authentication message by:

ascertaining at the target entity if the second authentication message has a length that exceeds the message length supported by the initiating entity; and either:

fragmenting the second authentication message into second message fragments if the length of the second authentication message exceeds the message length supported by the initiating entity; and either:

sequentially sending the second message fragments one by one across the Fabric to the initiating entity; or

sending the second authentication message in its entirety to the initiating entity if the length of the second authentication message is less than the message length supported by the initiating entity.

22. (Original) The method of claim 12, wherein the authentication message contains one or more of the following fields:

a field that identifies the authentication message as an authentication message; and

an authentication command code field that identifies the particular authentication message of an authentication protocol.

23. (Original) The method of claim 12, wherein the authentication protocol comprises, but are not limited to, one of the following protocols: DH-CHAP, SRP, or FCAP.